FAULT TREE ANALYSIS

A Special Bibliography from the NASA Scientific and Technical Information (STI) Program

FEBRUARY 2000

Fault tree analysis is a top–down approach to the identification of process hazards. It is touted as one of the best methods for systematically identifying and graphically displaying the many ways something can go wrong.

This sampler bibliography contains references to documents in the NASA STI Database. Selections are based on major concepts and NASA Thesaurus terms, including 'fault trees' and 'reliability analysis.' An abstract is included with most citations, followed by the applicable subject terms.

You may **order** one or more of the documents presented. For further details or questions, please call the NASA STI Help Desk at 301-621-0390 or send e–mail using the **comment form**.

19800064633
Uncertainty propagation in fault-tree analysis
Colombo, A. G., Commission of the European Communities, Joint Research Centre, Italy; Jan 1, 1980; 9p; In English; Synthesis and analysis methods for safety and reliability studies, July 3-14, 1978, Urbino, Italy; Sponsored by In: Synthesis and analysis methods for safety and reliability studies; Proceedings of the Advanced Study Institute; See also A80-48801 21-38; Copyright; Avail: Issuing Activity

Various methods for investigating the propagation of uncertainty from the lower level (primary event) to the higher level of a complex system in a fault-tree analysis are discussed with reference to a sample 750 failure mode fault-tree. It is shown that the problem of uncertainty analysis requires further research, particularly in the nuclear field where the error factor of failure parameter distribution is large. A numerical code which systematically combines random variables is found to be an efficient tool in this task, at least for numerical calculations.
AIAA
Complex Systems; Fault Trees; Probability Theory; Reliability Analysis; Stochastic Processes

19810002898 Science Applications, Inc., Advanced Power Systems Div., Palo Alto, CA, USA
Extension and validation of fault-tree analysis for reliability prediction
Land, R., Science Applications, Inc., USA; Rayes, L., Science Applications, Inc., USA; Burns, E. T., Science Applications, Inc., USA; Sep 1, 1980; 121p; In English
Report No.(s): EPRI-AP-1510; Avail: CASI; A06, Hardcopy; A02, Microfiche

The reliability projection for a type of fossil fueled power plant which makes use of a combustion turbine and heat recovery steam generator in parallel operation with a package boiler is presented. The fault tree methodology was used to estimate both the mean plant reliability plus a confidence interval for the calculated reliability prediction. The input component failure rates, including the error bounds were updated from an integrated data base obtained from the best available data. The estimated reliability results using a model representative of the initial two years of plant operation were compared with the reliability from plant operating experience data for a similar period, and these are presented. The estimated reliability for continuous plant operation for 500 hours is in good agreement with the plant operating experience. It is concluded that the fault tree methodology can be applied directly to both the qualitative and quantitative prediction of power plant reliability.
DOE
Electric Power Plants; Fault Trees; Prediction Analysis Techniques; Reliability Analysis

19810008957 Massachusetts Inst. of Tech., Energy Lab., Cambridge, MA, USA

Qualitative and quantitative reliability analysis of safety systems

Karimi, R., Massachusetts Inst. of Tech., USA; Rasmussin, N., Massachusetts Inst. of Tech., USA; Wolf, L., Massachusetts Inst. of Tech., USA; May 1, 1980; 288p; In English; Sponsored in part by Boston Edison Co., Mass.

Report No.(s): PB81-118325; MIT-EL-80-015; Avail: CASI; A13, Hardcopy; A03, Microfiche

A code was developed for the comprehensive analysis of a fault tree. The code designated UNRAC (UNReliability Analysis Code) calculates the following characteristics of an input fault tree: (1) minimal cut sets; (2) top event unavailability as point estimate and/or in time dependent form; (3) quantitative importance of each component involved; and (4) error bound on the top event unavailability. Overall it is demonstrated that UNRAC is an efficient, easy to use code and has the advantage of being able to do a complete fault tree analysis with this single code. Applications of fault tree analysis to safety studies of nuclear reactors are considered.

NTIS

Component Reliability; Computer Programs; Fault Tolerance; Fault Trees; Reliability Analysis

19810014944 Battelle Columbus Labs., OH, USA

Comparative analysis of techniques for evaluating the effectiveness of aircraft computing systems

Hitt, E. F., Battelle Columbus Labs., USA; Bridgman, M. S., Battelle Columbus Labs., USA; Robinson, A. C., Battelle Columbus Labs., USA; Apr 1, 1981; 156p; In English

Contract(s)/Grant(s): NAS1-15760

Report No.(s): NASA-CR-159358; Avail: CASI; A08, Hardcopy; A02, Microfiche

Performability analysis is a technique developed for evaluating the effectiveness of fault-tolerant computing systems in multiphase missions. Performability was evaluated for its accuracy, practical usefulness, and relative cost. The evaluation was performed by applying performability and the fault tree method to a set of sample problems ranging from simple to moderately complex. The problems involved as many as five outcomes, two to five mission phases, permanent faults, and some functional dependencies. Transient faults and software errors were not considered. A different analyst was responsible for each technique. Significantly more time and effort were required to learn performability analysis than the fault tree method. Performability is inherently as accurate as fault tree analysis. For the sample problems, fault trees were more practical and less time consuming to apply, while performability required less ingenuity and was more checkable. Performability offers some advantages for evaluating very complex problems.

S.F.

Fault Tolerance; Fault Trees; Reliability Analysis

19820056837

Analysis of reliability block diagrams by Boolean techniques

Bennetts, R. G., Cirrus Computers, Ltd., UK; IEEE Transactions on Reliability; Jun 1, 1982; R-31, pp. June 198; In English; p. 159-166; Copyright; Avail: Issuing Activity

A general purpose method for producing reliability expressions from reliability block diagrams based on an analysis of a pathset expression derived from the reliability block diagram is described. The resulting expression is tested for disjoitness and procedures are defined for making the terms disjoint if the test is failed. Unassigned variables are reintroduced into the terms in a manner which is consistent with an overall Boolean function and still guarantees disjointness. Relationships between Boolean and probabalistic algebras are explored and notation is defined, and the solution is found in terms of the test and modify algorithm without using a truth table. The method is concluded to be applicable to fault-tree analysis and general problems of reliability assessment, using only a hand calculator.

AIAA

Block Diagrams; Boolean Algebra; Fault Trees; Probability Theory; Reliability Analysis

19830039296

ESCAF - A new and cheap system for complex reliability analysis and computation

Laviron, A.; Manaranche, J. C., Commissariat a l'Energie Atomique, Centre d'Etudes de Valduc, Is-sur-Tille, France; Carnino, A., Commissariat a l'Energie Atomique, France; IEEE Transactions on Reliability; Oct 1, 1982; R-31, pp. Oct. 198; In English; p. 339-349; Copyright; Avail: Issuing Activity

A new apparatus, the electronic simulator to compare and analyze failures (ESCAF), is introduced as a means to analyze the reliability of systems with up to 416 components. ESCAF operates by simulating a system using the electronic gates of ICs mounted on specially configured cards. The component state is input and the failed or nonfailed state of the system is output after

a fault-tree analysis. A fault combination generator simulated the failure of all system components or the occurrence of all basic events, employing increasing orders of simulation until the most complex order of events is accounted for. Input of the individual event probabilities, component failure probabilities, or component unavailabilities yields computation of the overall system failure probability or unavailability. A serial transmission link is provided for interconnect with a mini- or microcomputer. Use of the device for spacecraft or nuclear power plant safety analyses is indicated.
AIAA
Electronic Equipment; Failure Analysis; Fault Trees; Reliability Analysis; Reliability Engineering; Systems Simulation

19830066397
Interval reliability for initiating and enabling events
Dunglinson, C., E.I. Du Pont de Nemours and Co., USA; Lambert, H.; IEEE Transactions on Reliability; Jun 1, 1983; ISSN 0018-9529; R-32, pp. June 198; In English; p. 150-163; Copyright; Avail: Issuing Activity

This paper describes generation and evaluation of logic models such as fault trees for interval reliability. Interval reliability assesses the ability of a system to operate over a specific time interval without failure. The analysis requires that the sequence of events leading to system failure be identified. Two types of events are described: (1) initiating events (cause disturbances of perturbations in system variables) that cause system failure and (2) enabling events (permit initiating events to cause system failure). Control-system failures are treated. The engineering and mathematical concepts are described in terms of a simplified example of a pressure-tank system. Later these same concepts are used in an actual industrial application in which an existing chlorine vaporizer system was modified to improve safety without compromising system availability. Computer codes that are capable of performing the calculations, and pitfalls in computing accident frequency in fault tree analysis, are discussed.
AIAA
Computer Aided Design; Fault Trees; Pressure Vessel Design; Reliability Analysis; System Failures; Systems Analysis

19830075603 Science Applications, Inc., Palo Alto, CA, USA
Verification of fault tree analysis. Volume 2: Technical descriptions
Rothbart, G., Science Applications, Inc., USA; Fullwood, R., Science Applications, Inc., USA; Basin, S., Science Applications, Inc., USA; Newt, J., Science Applications, Inc., USA; Escalera, J., Science Applications, Inc., USA; May 1, 1981; 167p; In English; Sponsored by EPRI
Contract(s)/Grant(s): EPRI PROJ. 1223
Report No.(s): DE81-903495; EPRI-NP-1570-VOL-2; Avail: CASI; A08, Hardcopy, Microfiche
Circuit Boards; Fault Trees; Printed Circuits; Reliability Analysis

19840063709
Fault tree analysis, taking into account causes of common mode failures
Stecher, K., Siemens AG, Germany; Siemens Forschungs- und Entwicklungsberichte; Jan 1, 1984; ISSN 0370-9736; 13, 4, 19; 8p; In English; Copyright; Avail: Issuing Activity

In evaluating fault trees using Boolean algebra and system function, subsystems can only be separated out if there are no failures of multiple-system components attributable to a common cause; i.e., so-called common-mode failures. For systems with distributed common modes, the effort required for this evaluation increases exponentially with the number of design components. This problem has been solved by means of a method in which the reliability data for the simple components are inserted on the lowest possible level of evaluation, whereas the data for the common modes are substituted at the top of the fault tree. The method described provides the basis for a computer program.
AIAA
Complex Systems; Failure Analysis; Failure Modes; Fault Trees; Reliability Analysis

19850027911
Safety analysis of Ada programs using fault trees
Leveson, N. G.; Stolzy, J. L., California, University, USA; IEEE Transactions on Reliability; Dec 1, 1983; ISSN 0018-9529; R-32, pp. 479-484; In English; Research supported by the University of California and Hughes Aircraft Co; Copyright; Avail: Issuing Activity

The technique of software fault-tree analysis (SFTA) is described using Ada as an example of a real-time programming language. It is shown that the system approach inherent in SFTA helps determine the safety requirements of the software. Thus, the preliminary system hazard analysis can be used to determine potential system hazards, and then the hazards can be traced back

to any potential software connection. Particular attention is given to the problems of concurrence and real-time constraints which are common in these types of applications.
AIAA
Ada (Programming Language); Computer Information Security; Fault Trees; Reliability Analysis; Software Engineering

19850064527
Fault tree analysis, methods, and applications - A review
Lee, W. S.; Grosh, D. L.; Tillman, F. A., Kansas State University, USA; Lie, C. H., Seoul National University, USA; IEEE Transactions on Reliability; Aug 1, 1985; ISSN 0018-9529; R-34, pp. 194-203; In English; Research supported by the Korea Science and Engineering Foundation
Contract(s)/Grant(s): N00014-76-C-0842; NSF INT-82-15755; Copyright; Avail: Issuing Activity

This paper reviews and classifies fault-tree analysis methods developed since 1960 for system safety and reliability. Fault-tree analysis is a useful analytic tool for the reliability and safety of complex systems. The literature on fault-tree analysis is, for the most part, scattered through conference proceedings and company reports. The literature has been classified according to system definition, fault-tree construction, qualitative evaluation, quantitative evaluation, and available computer codes for fault-tree analysis.
AIAA
Fault Trees; Reliability Analysis

19860036270
Fault-tree analysis using a binary decision tree
Schneeweiss, W. G., Fernuniversitaet, Germany; IEEE Transactions on Reliability; Dec 1, 1985; ISSN 0018-9529; R-34, pp. 453-457; In English; Copyright; Avail: Issuing Activity

A new algorithm for the production of a short disjoint-products form of a fault-tree output function is presented and discussed. This algorithm consists of a sequential binary decision process to find first big, then smaller sets of elementary system-failure states which correspond to disjoint-product terms. The identification of bad and good system states can be eased by a simple ternary (3-state) decision for which an auxiliary procedure is presented. The main advantages of this algorithm appear to be its efficiency, simplicity, and usefulness as an alternative (in the sense of multiversion programming for software fault tolerance) for the Shannon decomposition algorithm.
AIAA
Boolean Functions; Decision Theory; Fault Trees; Reliability Analysis; System Failures; System Identification

19880005868 Naval Postgraduate School, Monterey, CA, USA
Fault tree reliability analysis of the Naval Postgraduate School mini-satellite (ORION)
Keeble, Trenton G., Naval Postgraduate School, USA; Sep 1, 1987; 82p; In English
Report No.(s): AD-A186283; Avail: CASI; A05, Hardcopy; A01, Microfiche

Fault tree analysis, which has proved to be a useful analytical tool for the reliability and safety analysis of complex systems, is applied to the Naval Postgraduate School Mini-Satellite (ORION). A general background to reliability analysis, fault tree analysis, and fault tree construction is given. Impact of a phased mission is included in the analysis. A fault tree for ORION is constructed and used to identify minimal cut sets and minimal path sets. The cuts sets and path sets are, in turn, used to calculate an estimate of ORION's reliability to perform a three year mission. The reliability model was constructed in a Lotus 1-2-3 spreadsheet to enable the designers to do what-if analysis.
CASI
Computer Aided Design; Fault Trees; Reliability Analysis; Safety; Satellite Design

19880056132
Automated fault tree analysis via AI/ES
Kuzawinski, Karla M.; Smurthwaite, Richard, Xerox Corp., USA; Jan 1, 1988; 5p; In English; Annual Reliability and Maintainability Symposium, Jan. 26-28, 1988, Los Angeles, CA, USA; See also A88-43326; Copyright; Avail: Issuing Activity

A description is given of FTA, an interactive fault tree analysis tool that integrates the creation of fault trees with the propagation of failure rates. This tool allows the engineer to create, modify and manipulate fault trees easily, and requires little instruction on how to use the software. The fault trees generated are directly used in the propagation of failure rates without having to exit from the design environment. FTA software runs on a Xerox 1100 series workstation and is written in INTERSLIP-D. The

workstation has a large bit-mapped screen, and users interact with the workstation by input through a keyboard or selection by a mouse.
AIAA
Automatic Test Equipment; Expert Systems; Fault Trees; Maintainability; Reliability Analysis

19890001929 Sandia National Labs., Exploratory Batteries Div., Albuquerque, NM, USA
Reliability analysis of lithium cells
Levy, Samuel C., Sandia National Labs., USA; Bro, Per, Southwest Electrochemical Co., USA; Jan 1, 1988; 16p; In English; 4th; International Meeting on Lithium Batteries, 23 May 1988, Vancouver, British Columbia, Canada
Contract(s)/Grant(s): DE-AC04-76DP-00789
Report No.(s): DE88-009258; SAND-87-2129C; CONF-880598-2; Avail: CASI; A03, Hardcopy; A01, Microfiche

Fault tree analysis has been used for many years in safety and reliability analyses of nuclear reactors and other large systems. This technique can also be useful in the design of high reliability lithium cells/batteries and in improving the reliability of existing designs. The basic building blocks of a fault tree are discussed and an example, using the lithium-sulfur cell, is given.
DOE
Electrochemical Cells; Fault Trees; Reliability Analysis

19890059119 Texas Univ., Austin, TX, USA
Reliability database development for use with an object-oriented fault tree evaluation program
Heger, A. Sharif, Texas Univ., USA; Harringtton, Robert J., Texas Univ., USA; Koen, Billy V., Texas, University, USA; Patterson-Hine, F. Ann, NASA Ames Research Center, USA; Jan 1, 1989; 5p; In English; Annual Reliability and Maintainability Symposium, Jan. 24-26, 1989, Atlanta, GA, USA; See also A89-46451 20-38
Contract(s)/Grant(s): NSF DMC-86-15432; Copyright; Avail: Issuing Activity

A description is given of the development of a fault-tree analysis method using object-oriented programming. In addition, the authors discuss the programs that have been developed or are under development to connect a fault-tree analysis routine to a reliability database. to assess the performance of the routines, a relational database simulating one of the nuclear power industry databases has been constructed. For a realistic assessment of the results of this project, the use of one of existing nuclear power reliability databases is planned.
AIAA
Data Bases; Fault Trees; Nuclear Power Plants; Object Programs; Object-Oriented Programming; Reliability Analysis

19910007082 Edgerton, Germeshausen and Grier, Inc., Idaho Falls, ID, USA
Living PRAs (Probabilistic Risk Analysis) made easier with IRRAS (Integrated Reliability and Risk Analysis System)
Russell, K. D., Idaho National Engineering Lab., USA; Sattison, M. B., Idaho National Engineering Lab., USA; Rasmuson, D. M., Nuclear Regulatory Commission, USA; Jan 1, 1989; 33p; In English; 10th; International Conference on Structural Mechanics in Reactor Technology (SMIRT), 14-18 Aug. 1989, Anaheim, CA, USA
Contract(s)/Grant(s): DE-AC07-76ID-01570
Report No.(s): DE90-010938; EGG-M-89329; CONF-890855-60; Avail: CASI; A03, Hardcopy; A01, Microfiche

The Integrated Reliability and Risk Analysis System (IRRAS) is an integrated PRA software tool that gives the user the ability to create and analyze fault trees and accident sequences using an IBM-compatible microcomputer. This program provides functions that range from graphical fault tree and event tree construction to cut set generation and quantification. IRRAS contains all the capabilities and functions required to create, modify, reduce, and analyze event tree and fault tree models used in the analysis of complex systems and processes. IRRAS uses advanced graphic and analytical techniques to achieve the greatest possible realization of the potential of the microcomputer. When the needs of the user exceed this potential, IRRAS can call upon the power of the mainframe computer. The role of the Idaho National Engineering Laboratory of the IRRAS program is that of software developer and interface to the user community. Version 1.0 of the IRRAS program was released in February 1987 to prove the concept of performing this kind of analysis on microcomputers. This version contained many of the basic features needed for fault tree analysis and was received very well by the PRA community. Since the release of Version 1.0, many user comments and enhancements have been incorporated into the program providing a much more powerful and user-friendly system. This version is designated IRRAS 2.0. Version 3.0 will contain all of the features required for efficient event tree and fault tree construction and analysis.
DOE
Architecture (Computers); Computer Graphics; Fault Trees; Reactor Safety; Reliability Analysis; Risk

19920013534 Gates Aerospace Batteries, Gainesville, FL, USA

Fault tree analysis: NiH2 aerospace cells for LEO mission

Klein, Glenn C., Gates Aerospace Batteries, USA; Rash, Donald E., Jr., Reliability Analysis Center, USA; NASA. Marshall Space Flight Center, The 1991 NASA Aerospace Battery Workshop; Feb 1, 1992, pp. p 779-807; In English; See also N92-22740 13-44; Avail: CASI; A03, Hardcopy; A10, Microfiche

The Fault Tree Analysis (FTA) is one of several reliability analyses or assessments applied to battery cells to be utilized in typical Electric Power Subsystems for spacecraft in low Earth orbit missions. FTA is generally the process of reviewing and analytically examining a system or equipment in such a way as to emphasize the lower level fault occurrences which directly or indirectly contribute to the major fault or top level event. This qualitative FTA addresses the potential of occurrence for five specific top level events: hydrogen leakage through either discrete leakage paths or through pressure vessel rupture; and four distinct modes of performance degradation - high charge voltage, suppressed discharge voltage, loss of capacity, and high pressure.

CASI

Degradation; Electric Discharges; Fault Trees; Nickel Hydrogen Batteries; Reliability Analysis; Spacecraft Orbits; Spacecraft Power Supplies

19920051717 NASA Lewis Research Center, Cleveland, OH, USA

Structural system reliability calculation using a probabilistic fault tree analysis method

Torng, T. Y., NASA Lewis Research Center, USA; Wu, Y.-T., NASA Lewis Research Center, USA; Millwater, H. R., Southwest Research Institute, USA; Jan 1, 1992; 11p; In English; 33rd; AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics and Materials Conference, Apr. 13-15, 1992, Dallas, TX, USA; See also A92-34332

Contract(s)/Grant(s): NAS3-24389

Report No.(s): AIAA PAPER 92-2410; Copyright; Avail: Issuing Activity

The development of a new probabilistic fault tree analysis (PFTA) method for calculating structural system reliability is summarized. The proposed PFTA procedure includes: developing a fault tree to represent the complex structural system, constructing an approximation function for each bottom event, determining a dominant sampling sequence for all bottom events, and calculating the system reliability using an adaptive importance sampling method. PFTA is suitable for complicated structural problems that require computer-intensive computer calculations. A computer program has been developed to implement the PFTA.

AIAA

Fault Trees; Probability Density Functions; Reliability Analysis; Structural Failure; Structural Stability

19920073618

Approximate fault-tree analysis without cut sets

Schneeweiss, Winfrid G., Fernuniversitaet, Germany; Jan 1, 1992; 6p; In English; Annual Reliability and Maintainability Symposium, Jan. 21-23, 1992, Las Vegas, NV, USA; Sponsored by IEEE; See also A92-56201; Copyright; Avail: Issuing Activity

It is shown that a rather efficient approximate fault tree analysis is possible on the basis of the Shannon decomposition. The main advantages are: (1) no preprocessing is necessary to determine all the mincuts; (2) the maximum error can be prespecified; and (3) noncoherent systems and systems with dependent component states can be treated. The main disadvantage is the fact that the cutting off of certain subtrees of the decomposition tree (for upper bound results) may need some trial and error test calculations.

AIAA

Boolean Algebra; Fault Trees; Reliability Analysis

19930017833 NASA Lewis Research Center, Cleveland, OH, USA

Reliability studies of integrated modular engine system designs

Hardy, Terry L., NASA Lewis Research Center, USA; Rapp, Douglas C., Sverdrup Technology, Inc., USA; Jun 1, 1993; 19p; In English; 29th; Joint Propulsion Conference and Exhibit, 28-30 Jun. 1992, Monterey, CA, USA; Sponsored by AIAA

Contract(s)/Grant(s): RTOP 468-02-11

Report No.(s): NASA-TM-106178; E-7774; NAS 1.15:106178; AIAA PAPER 93-1886; Avail: CASI; A03, Hardcopy; A01, Microfiche

A study was performed to evaluate the reliability of Integrated Modular Engine (IME) concepts. Comparisons were made between networked IME systems and non-networked discrete systems using expander cycle configurations. Both redundant and non-redundant systems were analyzed. Binomial approximation and Markov analysis techniques were employed to evaluate total

system reliability. In addition, Failure Modes and Effects Analyses (FMEA), Preliminary Hazard Analyses (PHA), and Fault Tree Analysis (FTA) were performed to allow detailed evaluation of the IME concept. A discussion of these system reliability concepts is also presented.
Author
Engine Design; Failure Analysis; Failure Modes; Fault Trees; Modularity; Propulsion System Configurations; Reliability Analysis; Rocket Engine Design

19930065762 NASA Lewis Research Center, Cleveland, OH, USA

Reliability studies of Integrated Modular Engine system designs

Hardy, Terry L., NASA Lewis Research Center, USA; Rapp, Douglas C., Sverdrup Technology, Inc., USA; Jun 1, 1993, pp. 18 p.; In English; 29th; AIAA, SAE, ASME, and ASEE, Joint Propulsion Conference and Exhibit, June 28-30, 1993, Monterey, CA, USA; Sponsored by AIAA; Previously announced in STAR as N93-27022
Report No.(s): AIAA PAPER 93-1886; Copyright; Avail: Issuing Activity

A study was performed to evaluate the reliability of Integrated Modular Engine (IME) concepts. Comparisons were made between networked IME systems and non-networked discrete systems using expander cycle configurations. Both redundant and non-redundant systems were analyzed. Binomial approximation and Markov analysis techniques were employed to evaluate total system reliability. In addition, Failure Modes and Effects Analyses (FMEA), Preliminary Hazard Analyses (PHA), and Fault Tree Analysis (FTA) were performed to allow detailed evaluation of the IME concept. A discussion of these system reliability concepts is also presented.
Engine Design; Failure Analysis; Failure Modes; Fault Trees; Modularity; Propulsion System Configurations; Reliability Analysis; Rocket Engine Design

19940024900 NASA Lewis Research Center, Cleveland, OH, USA

Rocket engine system reliability analyses using probabilistic and fuzzy logic techniques

Hardy, Terry L., NASA Lewis Research Center, USA; Rapp, Douglas C., NASA Lewis Research Center, USA; Apr 1, 1994; 18p; In English; 30th; Joint Propulsion Conference, 27-29 Jun. 1994, Indianapolis, IN, USA; Sponsored by AIAA, ASME, SAE, and ASEE
Contract(s)/Grant(s): RTOP 506-42-72
Report No.(s): NASA-TM-106519; E-8640; NAS 1.15:106519; AIAA PAPER 94-2750; Avail: CASI; A03, Hardcopy; A01, Microfiche

The reliability of rocket engine systems was analyzed by using probabilistic and fuzzy logic techniques. Fault trees were developed for integrated modular engine (IME) and discrete engine systems, and then were used with the two techniques to quantify reliability. The IRRAS (Integrated Reliability and Risk Analysis System) computer code, developed for the U.S. Nuclear Regulatory Commission, was used for the probabilistic analyses, and FUZZYFTA (Fuzzy Fault Tree Analysis), a code developed at NASA Lewis Research Center, was used for the fuzzy logic analyses. Although both techniques provided estimates of the reliability of the IME and discrete systems, probabilistic techniques emphasized uncertainty resulting from randomness in the system whereas fuzzy logic techniques emphasized uncertainty resulting from vagueness in the system. Because uncertainty can have both random and vague components, both techniques were found to be useful tools in the analysis of rocket engine system reliability.
Author (revised)
Engine Failure; Fault Trees; Fuzzy Systems; Probability Distribution Functions; Reliability; Reliability Analysis; Rocket Engines

19950019625 Finnish Centre for Radiation and Nuclear Safety, Helsinki, Finland

Reliability analysis of software based safety functions

Pulkkinen, U., Technical Research Centre of Finland, Finland; May 1, 1993; 65p; In English
Report No.(s): DE95-606516; STUK-YTO-TR-53; Avail: CASI; A04, Hardcopy; A01, Microfiche

The methods applicable in the reliability analysis of software based safety functions are described in the report. Although the safety functions also include other components, the main emphasis in the report is on the reliability analysis of software. The check list type qualitative reliability analysis methods, such as failure mode and effects analysis (FMEA), are described, as well as the software fault tree analysis. The safety analysis based on the Petri nets is discussed. The most essential concepts and models of quantitative software reliability analysis are described. The most common software metrics and their combined use with software reliability models are discussed. The application of software reliability models in PSA is evaluated; it is observed that the recent software reliability models do not produce the estimates needed in PSA directly. As a result from the study some recommendations and conclusions are drawn. The need of formal methods in the analysis and development of software based

systems, the applicability of qualitative reliability engineering methods in connection to PSA and the need to make more precise the requirements for software based systems and their analyses in the regulatory guides should be mentioned.
DOE
Checkout; Computer Programs; Failure Analysis; Failure Modes; Fault Trees; Petri Nets; Qualitative Analysis; Quantitative Analysis; Reliability Analysis; Reliability Engineering; Software Reliability

19960000117 Naval Postgraduate School, Monterey, CA, USA
Fault isolator tool for software fault tree analysis
Mason, Russell W., Naval Postgraduate School, USA; Mar 1, 1995; 77p; In English
Report No.(s): AD-A294399; Avail: CASI; A05, Hardcopy; A01, Microfiche

Software fault tree analysis (SETA) is a technique used to analyze software for faults that could lead to hazardous conditions in systems which contain software components. A necessary element of a SETA process is the construction of software fault trees based upon the syntactical structure of the software being analyzed. The specific problem addressed by this thesis is how can the process of generating software fault trees based upon the translation of Ada source code files be automated. The approach taken to address this problem was to develop an automated tool that manipulates files created by the Automated Code Translation Tool (ACTT) developed earlier at the Naval Postgraduate School. The ACTT is an automated tool that translates Ada source code files into statement template tree structures that can be used to construct software fault trees. This thesis presents the Fault Isolator Tool (FIT), an automated process for locating and isolating those parts of a statement template tree structure generated by the ACTT tool that are related to statements in Ada programs that the analyst selects for evaluation. The FIT tool then generates software fault trees in a form compatible with the Fault Tree Editor (FTE), an interactive graphical editor developed for the display, editing, and evaluation of software fault trees.
DTIC
Ada (Programming Language); Fault Trees; Machine Translation; Program Verification (Computers); Reliability Analysis; Software Development Tools; Software Reliability

19980071382
Study of synthetic analysis on design reliablity of a liquid rocket engine
Kuang, Wuyue, Shaanxi Engine Design Inst., China; Tan, Songlin, Shaanxi Engine Design Inst., China; Journal of Propulsion Technology; Oct. 1997; ISSN 1001-4055; Volume 18, no. 5, pp. 9-12; In Chinese; Copyright; Avail: Aeroplus Dispatch

A synthetic analysis on the design reliability of a liquid rocket engine is presented. A rigorous yet practicable approach for evaluating engine reliability during the conceptual study phase is put forward. The approach uses the proven reliability methods of reliability modeling analysis, Failure Modes and Effects Analysis (FMEA), failure data analysis, and Fault Tree Analysis (FTA) to estimate the probability of mission success at the vehicle level for different engine designs. An example is provided in which the approach is used to evaluate an engine design concept.
Author (AIAA)
Liquid Propellant Rocket Engines; Rocket Engine Design; Reliability Analysis; Engine Failure; Fault Trees

19980117945
The service reliability analysis for the brake unit of a certain model aircraft
Fu, Changan, Air Force Aero College No. 2, China; Wang, Yuanda, Air Force Aero College No. 2, China; 1995, pp. 79-82; In English; Copyright; Avail: Aeroplus Dispatch

When aircraft of certain models land and the pilots brake, the service tire skidding and tire blowout are frequently occurring faults, endangering the landing safety. After having investigated and analyzed such incidents, the departments concerned think the fault is mainly caused by the improper brake operation when the aircraft lands. Using the fault tree analysis method, the paper first discusses the causes which result in severe tire skidding and blowout when the aircraft is braked, then presents some factors which the pilots and the ground crew should pay attention to in the actual use and maintenance work. Finally, improvements in the structure of the decelostat are proposed.
Author (AIAA)
Service Life; Reliability Analysis; Aircraft Brakes; Aircraft Models; Fault Trees; Skidding

19980148550
The fault tree analysis on system reliability on solid rocket motor design
Fang, Guoyao, Beijing Univ. of Aeronautics and Astronautics, China; Ma, Zhibo, Beijing Univ. of Aeronautics and Astronautics, China; Tang, Zhidong, Beijing Univ. of Aeronautics and Astronautics, China; Sun, Zhexi, Beijing Univ. of Aeronautics and

Astronautics, China; Journal of Propulsion Technology; Oct. 1994; ISSN 1001-4055, no. 5, pp. 28-33; In Chinese; Copyright; Avail: Aeroplus Dispatch

A fault tree analysis is carried out based on a real air-air missile solid rocket motor. Thus, the frame figure of system reliability, the fault tree analysis, and structure functions are developed, and the reliability is predicted. The results show that the model developed is correct and available for other solid rocket motors.

Author (AIAA)

Solid Propellant Rocket Engines; Fault Trees; Rocket Engine Design; Reliability Analysis

19980188713

Rocket engine system reliability analyses using probabilistic and fuzzy logic techniques

Hardy, Terry L., NASA Lewis Research Center, USA; Rapp, Douglas C., Sverdrup Technology, Inc., USA; Jun. 1994; In English Report No.(s): AIAA Paper 94-2750; Copyright; Avail: Aeroplus Dispatch

The reliability of rocket engine systems was analyzed by using probabilistic and fuzzy logic techniques. Fault trees were developed for Integrated Modular Engine (IME) and Discrete engine systems, and then were used with the two techniques to quantify reliability. The IRRAS (Integrated Reliability and Risk Analysis System) computer code, developed for the U.S. Nuclear Regulatory Commission, was used for the probabilistic analyses, and FUZZYFTA (Fuzzy Fault Tree Analysis), a code developed at NASA Lewis Research Center, was used for the fuzzy logic analyses. Although both techniques provided estimates of the reliability of the IME and Discrete systems, probabilistic techniques emphasized uncertainty resulting from randomness in the system whereas fuzzy logic techniques emphasized uncertainty resulting from vagueness in the system. Because uncertainty can have both random and vague components, both techniques were found to be useful tools in the analysis of rocket engine system reliability.

Author (AIAA)

Rocket Engines; Reliability Analysis; Fuzzy Systems; Logic Programming; Systems Integration; Fault Trees

19980192754

An assessment method for blade vibration reliability

Ou, Yangde, Beijing Univ. of Aeronautics and Astronautics, China; Kong, Ruilian, Beijing Univ. of Aeronautics and Astronautics, China; Song, Zhaohong, Beijing Univ. of Aeronautics and Astronautics, China; Journal of Aerospace Power; Apr. 1998; ISSN 1000-8055; Volume 13, no. 2, pp. 161-164; In Chinese; Copyright; Avail: Aeroplus Dispatch

A method is presented to assess the vibration reliability for blade design. The method, which is based on the Campbell diagram and the PFTA (Probability Fault Tree Analysis) concept, is used to improve conventional assessment methods and to develop an effective method for resonance identification and assessment of the characteristics of a blade resonance system that consists of multiple resonant interception on the Campbell diagram at or near the operating speed. This PFTA analysis is useful for improving the vibration characteristics of this blade and in eliminating blade failure from vibration fatigue.

Author (AIAA)

Structural Vibration; Turbine Blades; Fault Trees; Resonant Vibration; Aircraft Engines; Reliability Analysis

19990054676 Raytheon Systems Co., Fullerton, CA USA

Determining Software (Safety) Levels for Safety-Critical Systems

Tamanaha, Doris Y., Raytheon Systems Co., USA; Yin, Meng-Lai, Raytheon Systems Co., USA; Proceedings of the Twenty-Third Annual Software Engineering Workshop; June 1999; 43p; In English; See also 19990054657; Original contains color illustrations; No Copyright; Avail: CASI; A03, Hardcopy; A04, Microfiche

For safety-critical software-intensive systems, software (safety) levels are determined so that the appropriate development process is applied. This paper discusses issues of applying the results of fault tree analysis to software (safety) levels determination. In particular, the inconsistency problem, i.e., inconsistent software (safety) levels is addressed and an approach is presented.

Author

Computer Systems Programs; Fault Trees; Software Engineering; Software Reliability; Reliability Analysis; Consistency

19990056024

Fault-tree analysis of computer-based systems

Dugan, Joanne B., Virginia, Univ., Charlottesville, USA; 1999; In English; Copyright; Avail: AIAA Dispatch

This tutorial discusses several new and exciting approaches to fault tree analysis of computer-based systems. After a brief introduction to fault trees, we present an example analysis of a simple control system and then discuss the use of fault trees as a

design aid for software systems. The largest part of tutorial deals with methods for adapting the fault tree techniques to the analysis of computer-based systems. These methods include the incorporation of coverage models in the fault tree and the use of special gates for sequence dependencies. Several examples of fault tree models for computer systems are presented. These new techniques have allowed the fault tree model, long appreciated for its concise and unambiguous representational form, to be applicable to the analysis of complex fault-tolerant systems.
Author (AIAA)
Computer Techniques; Fault Trees; Reliability Analysis; Software Development Tools; Complex Systems

19990056049
Bridging the gap between systems and dynamic fault tree models
Manian, Ragavan, FORE Systems, Inc., USA; Dugan, Joanne B., Virginia, Univ., Charlottesville; Sullivan, Kevin J., Virginia, Univ., Charlottesville; Coppit, David W., Virginia, Univ., Charlottesville; 1999, pp. 105-111; In English
Contract(s)/Grant(s): NSF CCR-95-02029; NSF CCR-95-06779; NSF MIP-95-28258; Copyright; Avail: AIAA Dispatch

Fault tolerant systems are composed of subsystems that interact with each other, often in complex ways. Analyzing the reliability of these systems calls for sophisticated modeling techniques. One such technique is dynamic fault tree analysis. Because the semantics of dynamic fault trees are themselves complex, there is a question of whether such models are faithful representations of the modeled systems, and whether the underlying analysis techniques are correct. Previous definitions of the modeling constructs employed in dynamic fault trees were not precise or consistent enough, leading to ambiguities in their interpretation. We present our efforts at making the dynamic fault tree modeling and evaluation process precise. Our aim was to improve our confidence in the validity of dynamic fault tree models of system failure behavior. by rigorously specifying fault trees and their constituent gates and basic events, we were able to reason more effectively about the correctness of fault trees, the underlying analytical Markov models, and the numerical solution to these analytical models.
Author (AIAA)
Reliability Analysis; Fault Trees; Dynamic Models; Fault Tolerance; System Failures; Markov Processes

19990056056
Reliability analysis of complex hardware-software systems
Vemuri, Kiran K., Hewlett-Packard Co., USA; Dugan, Joanne B., Virginia, Univ., Charlottesville; 1999, pp. 178-182; In English; Copyright; Avail: AIAA Dispatch

We demonstrate how fault tree analysis could be used to perform reliability analysis of hardware-software systems. The functional dependence of the hardware components on the interfacing software components is appropriately modeled using fault trees. The Massachusetts Institute of Technology Center for Space Research Advanced X-ray Astrophysics Facility Imaging Charge Couple Device Imaging Spectrometer (ACIS) system is used to illustrate the fault tree analysis method in reliability analysis of complex hardware-software systems. The ACIS science instrument system is a spaceborne system to acquire and process X-ray images over the sky, and sends them to Earth. It has hardware and software components with interfaces between them, making it a very good example of a complex hardware-software system. This approach could be used in analyzing other complex systems being designed today and in identifying the critical components to make the system safe and more reliable.
Author (AIAA)
Reliability Analysis; Software Reliability; Hardware; Fault Trees; X Ray Imagery